

CYBER
THREAT
ANALYSIS

Recorded Future®

Insikt Group®

2022년 5월 24일



사기 비즈니스: 금융 사기 보고서



주요 내용

오늘날 위협 행위자들은 금융 기록 조작, 대출 승인, 대출 신청 정보가 포함된 계정 구매 방법에 대한 안내서와 서비스를 판매하고 있다. '해커 임대(Hackers For Hire)' 서비스에는 기록 및 문서에 액세스하고 조작하는 작업까지 포함된다.

위조 수표는 여전히 수요가 높으며 흔히 송금 또는 현금 인출 시도와 연계된다. 위조 수표 생성 수단은 한층 자동화되고 맞춤화되었으며, 위협 행위자는 이 서비스를 중심으로 상점을 운영하며, 따라하기 쉬운 사용자 인터페이스를 제공한다.

위협 행위자는 인스턴트 메시징 플랫폼을 사용하여 수표, 대출, 송금, 회계 사기를 위한 서비스와 목록을 광고하고 판매한다. 이러한 메시징 플랫폼은 기존의 다크웹 생태계(포럼, 시장 및 상점)에 비해 즉각적인 커뮤니케이션을 제공하고, 목록 추가 및 제거가 훨씬 용이하고, 누구나 쉽게 접근할 수 있다는 점에서 광범위하게 활용되고 있다.

배경

금융 사기는 부당한 방식으로 금융 기관이 소유하거나 보유하고 있는 금전, 자산 또는 기타 재산을 획득하거나 은행 또는 기타 금융 기관을 사칭하여 예금자로부터 돈을 탈취하는 것이다. 금융 사기법의 구체적인 요소는 관할 지역에 따라 다르지만 "금융 사기(Bank Fraud)"라는 용어는 은행 강도나 물리적 절도와는 달리 계획된 설계나 기법을 사용하는 행위에 적용된다. 이러한 이유로 금융 사기는 종종 화이트칼라 범죄로 간주된다. 오늘날 고객은 온라인 बैं킹 서비스를 통해 개인용 컴퓨터와 모바일 기기로 금융 계좌와 기록에 액세스할 수 있다. 이러한 편리함은 공격 노출면을 증가시켰을 뿐만 아니라 사이버 범죄자들이 기존 수법과 새로운 수법을 창의적으로 활용하여 불법을 자행할 수 있도록 해주었다.

레코디드 퓨처는 2021년 3월부터 2022년 3월까지 레코디드 퓨처 플랫폼, 다크웹, 특수 인가 소스, OSINT(open-source intelligence) 데이터를 분석하여 위협 행위자(Threat Actor)가 회계, 대출, 수표, 전신송금 유형의 금융 사기를 실행하고 광고하는 방법을 관찰하고 파악했다. 이 보고서는 *Insikt Group Fraud Series* 첫 번째 보고서 "[사기 비즈니스: 사이버 범죄의 수익 창출 방식\(The Business of Fraud: An Overview of How Cybercrime Gets Monetized\)](#)"에 이은 후속 보고서이다.

개요

금융 사기는 부당한 방법을 사용하여 은행, 금융 기관 또는 다른 개인으로 위장하고 금융 기관이나 개인이 소유하고 있는 금전, 자산 또는 기타 재산을 탈취하는 것이다. 온라인 및 인터넷 बैं킹이 금융 비즈니스 모델에 통합됨에 따라 은행에서 금전을 탈취하는 전통적인 사기 수법이 오늘날의 온라인 बैं킹 직원과 소비자를 타겟으로 복제되고 업데이트되었다. 레코디드 퓨처는 "사기 비즈니스(Business of Fraud)" 보고서 시리즈를 통해 사이버 범죄자가 온라인 범죄 활동을 위해 사용하는 다양한 TTP(tactics, techniques, and procedures)를 파악했다. 노출된 개인식별정보(Personally identifiable information, PII) 수집, 사용에서 사회 공학에 이르기까지 이러한 TTP 중 상당수가 금융 및 온라인 बैं킹 계정 사기를 자행하는 데 사용되고 있다. 이 보고서에서 우리는 회계, 대출, 수표, 송금(accounting, loan, check, and wire transfer) 유형의 금융 사기와 관련된 사이버 범죄 수법을 조사하고 종종 간과되고 다른 유형의 금융 관련 사기와 유사점을 확인하였다.

위협 행위자는 피싱, 자격증명 재사용, 멀웨어 또는 다크웹 구매를 통해 훔친 ID를 사용하거나(계정 도용, identity theft), 신규 계정을 개설하거나(신청 사기, application fraud), 기존 계정에 대한 유효 자격 증명을 획득(계정 탈취, account takeover)하는 등의 다양한 방법으로 온라인 뱅킹 계정에 액세스한다. 레코디드 퓨처의 이전 보고서에서 금융 범죄(자금 세탁, 해킹한 PII 및 위조 문서를 사용한 계좌 개설, 스니퍼 사용, 뱅크 인젝트/오버레이(bank injects/ overlays), 인포스틸러(Infostealers)로 금융 자격증명을 수집하여 계좌 및 신용카드 탈취, 운반책 모집 및 현금 인출 서비스에 대해 다루었으므로 이 보고서는 노출된 결제 카드 데이터 또는 앞서 언급한 주제 중 하나에 특별히 초점을 맞추지 않을 것이다. 그보다 이 보고서에서는 사이버 범죄자들이 일반적으로 덜 알려져 있는 금융 사기(수표, 대출, 송금, 회계 사기)를 획책하기 위해 다양한 다크웹 및 특수 인가 소스에서 작업을 수행하는 방법을 조사한다.

금융 사기 유형

레코디드 퓨처의 “사기 비즈니스(Business of Fraud)” 보고서 시리즈에서 중점적으로 다루는 부분은 위협 행위자가 금융 사기를 지원하는 데 사용하는 TTP이다.

- 대부분의 위협 행위자는 이 보고서에서 언급된 4가지 유형의 금융 사기 서비스에 대해 특별히 광고하지 않는다. 오히려 다른 유형의 금융 사기에 이러한 활동을 결합하여 포함시킨 서비스 및 수단을 제공하고 있다.
- 대부분의 사기 유형과 마찬가지로 계정 생성이나 제어에 필요한 유출된 자격 증명과 PII가 금융 사기의 핵심이다. 위협 행위자는 다른 사이버 사기 범죄에 사용되는 동일한 포럼, 마켓플레이스, 상점(판매자 및 구매자 모두)을 통해 이러한 데이터를 광고하고 있다.

위협 행위자들은 최근 여러 개인의 소유 PII(생년월일, 주민등록 번호 등)를 결합하여 하나의 새로운 ID를 만드는 사기 ID 유형인 SID(Synthetic Identity)에 관심을 갖고 있다. 이 보고서에서는 SID에 대해 구체적으로 다루지 않지만, 방대한 양의 유출된 PII 데이터와 사기 수법(사회 공학, 피싱, 기타) 정보가 다크웹에서 널리 공유되고 있음을 고려하면 이 공격 벡터가 향후 범죄자들에게 매력적인 전술이 될 것으로 보인다. 특히 은행 및 금융 관련 범죄에서 계좌 개설이나 대출 신청 수단이 될 수 있다. 레코디드 퓨처 데이터 세트에 따르면 다양한 다크웹과 특수 인가 소스에 SID 생성 방법에 대한 다수의 튜토리얼과 가이드가 올라와 있다.

수표 사기

수표 사기(Check Fraud)는 은행 수표를 불법적으로 사용하여 계좌 소유자의 자금을 탈취하는 것을 의미한다. 위조 수표는 기업 또는 개인 수표, 캐시 수표 또는 전자 수표 등의 다양한 형태로 악용된다. 사기가 끊임없이 진화하고 기술이 크게 발전함에 따라 소비자는 물론 은행 직원도 식별하기 어려운 위조 수표와 우편환이 제작 가능해졌다. 또한 최근 모바일 앱을 통해 수표를 입금하거나 온라인으로 입금하는 등의 서비스가 널리 보급되면서 은행 고객은 물론 사기꾼의 생활도 편리해졌다.

이러한 활동의 예로는 Verified Forum의 회원인 "Fogel 2010"이 게시한 광고가 있다. 2021년 8월 11일 Fogel 2010은 수표를 인쇄할 수 있는 미국 내 파트너를 찾는 게시물을 작성했는데, 이는 미국 은행과 피해자를 노렸음을 나타낸다. 사이버 범죄자는 수표를 자신의 온라인 은행 계좌에 입금하거나 또는 위조 수표를 본인 은행 계좌에 입금한 후 현금으로 인출할 수 있는 공범자를 통해 수표를 현금화할 수 있다. 이 보다 앞선 2019년 10월에 Fogel 2010은 2,000달러에서 5,000달러 사이의 금액으로 미국 기업 수표를 현금으로 바꿀 수 있는 인출책을 찾는 광고를 게재했다. 그림 1과 2는 이러한 게시물을 보여준다.



그림 1, 2: 현금화를 위해 수표를 인쇄할 수 있는 파트너를 모집하고 있는 Fogel 2010 (출처: Verified Forum).

범죄자는 위조 수표를 생성하는 서비스를 사용할 수도 있다. 예를 들어 ScanLab이라는 다크웹 상점은 고객이 원하는 은행, 수표 유형, 금액으로 위조 수표를 만들어준다. 또한 ID 카드, 운전면허증, 사회보장카드 등과 같은 위조 문서 생성 서비스도 제공한다.

대출 사기

대출 사기(Loan Fraud)를 위해 범죄자는 대출 기록 및 신청서 정보를 위조한다. 다른 종류의 사기들과 마찬가지로 이제 많은 위협 행위자가 대출 사기 서비스를 제공한다. 지불 카드 사기, [세금 사기](#), 실업 사기와 같은 다른 유형의 사기에 쓰이는 유사한 수법이 사용될 수 있다. 그러나 레코디드 퓨처의 분석에서 대출 사기 수법에 관심이 있는 사용자의 수요가 대출 사기 관련 서비스 및 목록을 제공하는 위협 행위자의 공급보다 더 높게 나타났다.

대출 사기를 피하는 위협 행위자는 모기지, 학자금 대출을 비롯한 모든 유형의 대출과 관련된 애플리케이션 기법과 서비스에 관심을 갖는다. 위협 행위자는 다크웹과 특수 인가 소스를 통해 훔친 PII와 민감한 데이터 뿐만 아니라 대출 사기 수행 방법, 신청서 작성 서비스, 액수에 따라 즉시 구매 가능한 대출을 마음대로 사용할 수 있다. 이러한 활동의 대부분은 하위 포럼 및 마켓플레이스에서 발생한다. 위협 행위자 서비스 및 가이드 목록 샘플은 표 1에 나와 있다.

위협	행위자	소스	정보
"fraudbuddy"	Hermes Market		2022년 3월, 위협 행위자가 대출 신청이 포함된 금융 사기 수법 튜토리얼을 100달러에 판매한다고 올렸다. 위협 행위자는 해당 튜토리얼을 구매하면 직통 개인 연락처를 제공하고 신청 절차 진행에 도움을 주겠다고 광고했다. 위협 행위자는 다양한 다크 웹 마켓플레이스에 동일하고 유사한 사기 수법을 올려놓고 있다.
"ESCO"	Carders.ws		이 위협 행위자는 2020년 11월부터 현재까지 은행 대출을 포함한 대출 취득 및 승인 방법에 대한 자습서를 제공하고 있다. 해당 가이드와 교육을 받은 포럼 사용자들이 긍정 평가를 제공했다.
"kaki09"	Altenen		2021년 9월, 이 위협 행위자는 대출 사기 수법을 올렸다. 이 위협 행위자는 현금 인출 및 기타 유형의 금융 관련 사기를 비롯한 다양한 사기 방법을 빈번하게 게시한다.

표 1: 대출 사기 서비스를 제공하는 위협 행위자의 샘플 목록 (출처: Recorded Future)

위협 행위자들은 또한 대출 신청 정보와 지불금이 나와있는 해킹된 계정에 대한 액세스와 같은 금융 관련 데이터 판매를 전문으로 하는 다크웹 상점을 사용하고 있다. 이와 같은 유형의 유출된 정보 목록은 다크웹 생태계에만 국한되지 않고 상점처럼 운영되는 공개적으로 액세스 가능한 텔레그램 채널에도 올라온다. 이러한 채널 중 일부는 다수의 공급업체를 호스팅하며 해킹된 금융 데이터를 판매한다. 여기에는 다양한 채널에서 대출 관련 상품을 판매하는 160개 이상의 공급업체들이 포함된다.

Boobie Brown

🔥 DM FOR ALL YOUR LOAN GUIDE 🔥

ESCRIPT METHOD
 BOA GLITCH WAVE
 VENMO GLITCH WAVE
 APPLE BANK LOAN
 SIM SWAP TUTORIAL
 TAX SLAYER WAVE
 SANTANDER BANK LOAN
 WELLS FARGO LOAN
 CALI EDD TUTORIAL
 NEW SBA TUTORIAL
 WASHINGTON DC RENTAL ASSISTANCE
 EMV SOFTWARE
 12 PRO MAX CARDING AT&T
 MSR READER/ SOFTWARE
 NEW JERSEY TUTORIAL
 MISSOURI RENTAL SAUCE
 COINBASE LOADING TUTORIAL
 SDI TUTORIAL
 LOUISIANA GRANT
 FLORIDA RELIEF LOAN
 NEW YORK WORKERS LOAN
 HOW TO CHECK CREDIT SCORE
 APPLE PAY SAUCE
 BANK OPEN UPS
 TAX REFUND 2022
 NEVADA UNEMPLOYMENT TUT
 CASHAPP METHOD
 TREASURY GRANT SAUCE
 SPAMMING VIDEO TUTORIAL
 CARDING FOR BEGINNERS
 BEST BUY TUTORIAL

@SDK242

그림 3: 공개 채널에 올라온 "SDK242"의 은행 및 기업 대출 가이드 목록 (출처: Telegram)

송금 사기

사이버 범죄자에게 송금 사기(Wire Transfer Fraud)의 매력은 일단 송금이 이루어지면 취소가 매우 어렵거나 불가능하다는 점이다. 일반적으로 금융 사기를 치기 위해 사이버 범죄자는 피해자의 은행 계좌에 액세스하여 자신이 통제하는 계좌(또 다른 도난 계좌일 수도 있음)로 계좌 이체를 한 다음 자금을 인출해야 한다. 은행 송금의 한 가지 어려움은 은행이 송금인의 신원을 확인할 수 있으므로 사이버 범죄자가 피해자의 PII와 경우에 따라 위조 문서를 확보해야 한다는 점이다.

위협 행위자는 [포럼](#), [시장](#), [메시징 플랫폼](#)을 사용하여 송금 사기 방법 가이드, 전송/수신/현금화가 포함된 송금 사기 서비스, 송금 요청 방법 가이드 등의 송금 사기 서비스와 제품을 광고한다. 사이버 범죄자들은 텔레그램을 갈수록 애용하고 있다. 텔레그램이 제공하는 익명성, 폭넓은 고객 기반(다크웹 액세스 경우와 같은 특수 소프트웨어가 필요 없음) 덕분에 자신의 상점을 더 쉽게 운영하면서 원활한 통제(목록 추가 또는 삭제, 사용자 제거 또는 차단 등) 또한 가능하기 때문이다. 이러한 채널은 대부분 노출을 극대화하기 위해 공개적으로 운영된다. 일부 채널은 다수의 판매자를 호스팅하여 경쟁적으로 연중무휴 24/7 고객 서비스와 판매가 이루어지게끔 한다.

Bank transfer will take a maximum 6hour to show money in your bank account.

∞ TRANSFER RATES ,

\$500 Transfer = \$50
 \$1000 Transfer = \$100
 \$2000 Transfer = \$200
 \$3000 Transfer = \$300
 \$4000 Transfer = \$400
 \$5000 Transfer = \$500
 \$6000 Transfer = \$600
 \$7000 Transfer = \$700
 \$8000 Transfer = \$800
 \$9000 Transfer = \$900
 \$10000 Transfer = \$1000

Western Union Transfer Available To All Country Inbox Me Now Let Make Some Cash Together On Here Hit me up for long term business.

\$150 BTC -> \$1500 WU TRANSFER
 \$200 BTC -> \$2000 WU TRANSFER
 \$250 BTC -> \$2500 WU TRANSFER
 \$300 BTC -> \$3000 WU TRANSFER
 \$400 BTC -> \$4000 WU TRANSFER
 \$500 BTC -> \$5000 WU TRANSFER

INFO NEEDED FOR TRANSFER:

- 1: FULL NAME
- 2: CITY
- 3: COUNTRY
- 4: VALID EMAIL FOR SENDING YOU MTCN INFO

그림 4: "[Trusted] Panda" (@TrustedPanda) 송금 서비스 및 요금 (출처: Telegram)

위협 행위자가 금융 활동을 은폐하기 위한 방법으로 선택하는 또 다른 서비스는 국제 제재를 우회하고 금융 정보 또는 계좌 정보를 미국 또는 기타 국가에 누설하지 않는 역외 은행 및 기관을 사용하는 것이다. 이러한 방식은 2021년 말 [판도라 페이퍼\(Pandora Papers\)](#)가 공개되면서 주목을 받게 되었다. 또한 2022년 2월 러시아의 우크라이나 침공 이후 미국과 서유럽 국가들의 [경제 및 금융 제재](#)를 피해 러시아인들이 제재에 협조하지 않는 국가로 자금을 [송금](#)하려고 하면서 새로운 관심을 받고 있다.

Accounts available for international wire transfer, Hongkong, Thailand, Singapore, European and USA accounts available.
 No online access available.
 Can receive funds from any country.
 payment, No time wasting messages plz only serious and long term individual/organization required.

Post 1 of 1 by Dbluebird on Jan 31 2022, 07:53

그림 5: 역외금융 거래처 송금 서비스 (출처: Recorded Future)

레코디드 퓨처는 역외금융(offshore banking)에 대한 정보, 특히 은행 선택 방법이나 최적의 국가, 모범 사례 등을 게시하는 지금은 없어진 Raid Forums에서 포럼 사용자 "kith"를 식별했다. 이러한 포럼은 유출된 데이터의 판매 뿐만 아니라 인텔리전스를 공유하는 수단으로도 사용된다. 이러한 공유가 동질성과 신뢰를 구축하고 커뮤니티를 강화하기 때문이다. 역외 계좌를 개설하거나 자금을 송금하는 기관 이름이 구체적으로 언급되지 않았지만, 우리는 위협 행위자들이 특히 메시징 플랫폼을 통해 홍콩이나 싱가포르와 같은 인기 있는 국가의 국제 은행 계좌 역외금융 서비스를 광고하는 것을 확인했다.

이러한 서비스는 흔히 커스터마이징 가능한 형태로 제공된다. 위협 행위자는 은행 송금 서비스를 사용하여 역외 은행으로 자금을 송금하는 것을 포함하여 고객의 특정한 요청에 기꺼이 협력한다.

회계 사기

회계 사기(Accounting Fraud)는 이익을 숨기거나 손실을 은폐하거나 회사의 실제 재무 상태를 알기 어렵게 만들기 위해 회사 재무 기록을 고의적으로 변경하는 것이다. 오늘날 디지털 세상에서는 위협 행위자가 자신이 통제하는 계좌로 자금 이체 및 지출을 실행하기 위해 계좌 정보를 변경하는 행위도 확장된 회계 사기에 포함된다. 레코디드 퓨처 조사에서 회계 사기 서비스를 제공한다고 광고하는 특정 위협 행위자는 파악되지 않았다. 그보다는 위협 행위자가 문서 조작을 목적으로 회사 재무 기록에 액세스하도록 해주는 해킹 서비스, 내부자 위협, 네트워크 침투가 파악되었다.

지난 해 레코디드 퓨처는 다양한 다크웹 포럼에서 해킹 서비스를 광고하는 위협 행위자들을 파악했다. 이러한 서비스는 기록 변경, 신용 등급 업그레이드, 요청에 따른 맞춤형 서비스를 비롯한 다양한 기능을 포함한다. 광고의 대부분이 Card Villa, Carding Mafia와 같은 유출된 카드 정보 관련 포럼에서 발견되었지만 Hack This Site 및 XSS Forum과 같은 포럼에도 이러한 서비스에 대한 게시물이 올라왔다. 이들 서비스 중 상당수가 해커가 고객의 특정 요청, 요구, 기대치에 맞춰 제공하는 맞춤형 서비스였다.

이러한 해킹 서비스 외에도 레코디드 퓨처는 작년에 Citrix, RDP(remote desktop protocol), 웹 셸(web shell) 등과 같은 다양한 유형의 네트워크 액세스를 광고하고 판매하는 90건 이상의 위협 행위자 개별 사건에 대해 보고했다. 이러한 형태의 액세스는 흔히 멀웨어 및 랜섬웨어 감염과 관련이 있지만, 적극적인 위협 행위자는 이러한 액세스 수단을 사용하여 기업의 회계 부서 권한을 얻고 회계 문서와 기타 민감한 회사 기록을 획득하여 변조할 수도 있다. 2022년 4월 위협 행위자 "mavro5220"이 한 캐나다 은행에 대한 액세스를 판매한다고 올렸다. 이 액세스가 계좌 번호 변경이 가능한 취약점과 결합되는 경우(예: 2021년 12월 "Brady"의 목록은 계좌 번호를 변경할 수 있다고 주장), 위협 행위자는 자신의 통제 하에 있는 계좌로 자금이 전송되도록 계좌 번호와 기타 민감한 정보를 변경할 수 있다.

모든 네트워크 침입이 파괴적인 것은 아니다. 의도를 가진 위협 행위자는 탐지되지 않은 상태로 네트워크 내에 계속 숨어있는 멀웨어를 사용하여 기업을 공격할 수 있다. 탐지되지 않은 상태로 남아 있으면 위협 행위자가 자금과 데이터를 자신이 통제하는 계정으로 전송하는 데 사용할 수 있는 회계 기록과 기밀 재무 데이터를 빼돌릴 수 있다. Insikt Group이 이전에 보고한 바와 같이 위협 행위자는 피싱 또는 BEC(business email compromise)와 같이 다양한 측면으로 사회 공학을 활용하여 피해자의 네트워크에 액세스한다. 이러한 유형의 공격은 탐지 메커니즘이나 직원 보안 교육이 미흡한 중소기업에 피해를 입히는 경우가 많다. Insikt Group의 조사 결과를 기반으로 레코디드 퓨처는 침투 및 스파이 활동을 위해 주로 원격 액세스 툴과 RAT(remote access trojans)를 배포하는 위협 행위자를 식별했다. 지난 해 레코디드 퓨처 데이터 세트는 위협 행위자가 피싱 이벤트에 KONNI, PlugX, REMCOS RAT, Cobalt Strike, Revenge RAT와 같은 원격 액세스 도구와 RAT를 사용한다는 것을 보여주었다.

마지막으로 무심결에 멀웨어를 다운로드하는 내부자부터 고급 정보를 얻기 위해 프로토콜을 의도적으로 위반하는 악의적인 내부자에 이르기까지 내부자 위협도 회계 사기를 수행하는 수단이 된다. 2021년 6월 남아프리카 은행 Postbank의 직원이 데이터 센터에서 암호화되지 않은 플레인 텍스트(키 소유자가 계좌 잔액에 액세스하고 조작할 수 있음)로 된 은행의 **마스터 키를 훔쳐** 최소 25,000건의 사기 거래가 발생했다. 또한 지능형 위협 그룹이 회계 관련 시스템과 문서에 대한 액세스 권한을 얻기 위해 내부자를 모집할 수 있다. 금전적 이익을 노리는 지능형 위협 그룹 FIN7은 정통 IT 회사를 사칭하여 **전문가를 모집**하고 GRIFFON 멀웨어가 포함된 **감염된 USB 드라이브를 우편으로 발송**하여 악성 작업을 확산을 시도했다.

향후 전망

이 보고서에서 다룬 4가지 유형의 금융 사기는 서로 다른 유형의 사기가 유사한 방식을 사용하고 유사한 데이터를 필요로 함을 보여준다. 금융 관련 사기의 대부분은 유출된 결제 데이터 및 계정과 관련되기 때문에 해킹된 PII 데이터 및 우회 수단은 다른 형태의 사기 외에도 회계, 대출, 수표, 송금 사기 유형에 두루 사용된다. 이러한 유형의 사기는 다크웹 범죄 생태계 전반에서 많은 수요를 기반으로 활발히 광고되고 있다. 위협 행위자는 서비스와 제품의 광고, 토론, 검색, 판매를 위한 수단에 계속해서 암호화된 인스턴트 메시징 플랫폼을 통합하고 있다.

레코디드 퓨처의 2020 시리즈에서 다크웹의 **자동화 맞춤화** 서비스를 조명한 것처럼 이 보고서에서 주목한 위협 행위자들 역시 끊임없이 서비스를 맞춤화하고, 간편한 인터페이스의 자동화된 상점과 마켓플레이스를 호스팅하고, 공격 벡터를 업데이트하여 보안 조치를 무력화시킨다. 레코디드 퓨처는 위협 행위자가 고객 유치와 수익 창출을 위해 계속해서 비즈니스 모델에 자동화와 맞춤화를 통합할 것으로 판단한다. 이러한 서비스에 대한 수요는 줄어들 기미가 보이지 않으므로 레코디드 퓨처를 통해 자사 브랜드에 영향을 미칠 수 있는 이벤트 또는 위협 행위자 판매 목록에 대한 업데이트와 알림을 적시에 받을 것을 권장한다. 경고가 수신되면 심각도를 분류하고 레코디드 퓨처와 협력하여 보안 조치 강화를 위해 앞으로 취해야 할 솔루션과 단계를 파악하도록 한다.

Insikt Group®

레코디드 퓨처의 위협 연구 부서인 Insikt Group은 정부, 법 집행 기관, 군 기관, 정보 기관 경험이 풍부한 분석가와 보안 연구원으로 구성되어 있다. Insikt Group의 임무는 고객의 위협을 줄이고 실질적인 결과를 제공하며 비즈니스 중단을 방지하는 인텔리전스를 제공하는 것이다. 연구 영역에는 국가 차원 위협 그룹, 금전적 이익을 위해 다크넷에서 활동하는 위협 행위자, 지하 범죄조직, 최신 멀웨어 및 공격자 인프라, 전략적 지정학적 정보, 군사 작전 등이 포함된다.

레코디드 퓨처에 대하여

레코디드 퓨처(Recorded Future)는 세계 최대 엔터프라이즈 보안 인텔리전스 제공업체이다. 레코디드 퓨처는 지속적이고 광범위한 자동 데이터 수집 및 분석에 전문가 분석을 결합하여 적시에 정확하고 실행 가능한 인텔리전스를 제공한다. 레코디드 퓨처는 끊임없이 증가하는 혼란과 불확실성의 세계에서 조직이 위협을 신속하게 파악하고 탐지하는 데 필요한 가시성을 제공한다. 조직은 이러한 가시성을 확보함으로써 선제적 대응을 통해 공격을 저지하고 사용자, 시스템, 자산을 보호하여 비즈니스를 안정적으로 수행할 수 있다. 레코디드 퓨처는 전 세계 1,000개 이상의 기업과 정부 기관에서 신뢰받고 있다.

자세한 사항은 www.recordedfuture.com과 Twitter @RecordedFuture에서 확인할 수 있다.